EP 28324

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification⁷: H04Q 7/00

(21) International Application Number: PCT/EP01/08856

(22) International Filing Date: 31 July 2001 (31.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0020443.8   18 August 2000 (18.08.2000)   GB

(71) Applicant (for all designated States except US): NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and
(75) Inventors/Applicants (for US only): ISOKANGAS, Jari [FI/FI]; Itsenäisyydenkatu 8 C 43, FIN-33500 Tampere (FI). SARKKINEN, Sinikka [FI/FI]; Kisällinkuja 5, FIN-36200 Kangasala (FI).

(74) Agents: RUUSKANEN, Juha-Pekka et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— without international search report and to be republished upon receipt of that report

[Continued on next page]

(54) Title: CONTROLLING COMMUNICATIONS BETWEEN STATIONS

(57) Abstract: The present invention relates to relocation of the control of communication between a first station and a second station from a first communication system controller to a second communication system controller. The communication is ciphered by means of a first ciphering key. In the method, after the initiation of the relocation of control of the communication from the first controller to the second controller a request for relocation is transmitted to the second controller. The request contains the first ciphering key and at least one other ciphering key.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

1

Controlling communication between stations

Field of the Invention

5   The present invention relates to communication system and in particular, but not
exclusively, to relocation of functions controlling ciphered communications
between stations from a first controller to a second controller.

Background of the Invention

10

Communication networks typically operate in accordance with a given standard or
specification which sets out what the elements of the network are permitted to do
and how that should be achieved. The communication in the networks typically
follows predefined rules which are referred to in the following as protocols. The

15   protocols to be used are defined in the associated standards or specifications. The
protocols can be used for transmission of necessary control information between
the various network elements.

A communication network is a cellular radio network consisting of access entities
20   referred to as cells. In most cases the cell consists of a certain radio access area
covered by one or several base transceiver stations (BTS) serving mobile stations
(MS) via a radio interface and connected to a base station subsystem (BSS).
Several cells cover a larger area, and form the coverage area of a cellular radio
network. The cell (or group of cells) and thus the mobile station (MS) (that is
25   sometimes referred to as user equipment UE) within one of the cells of the system
can be controlled by a node providing control function. An example of such
controller is a radio network controller (RNC) of a universal mobile
telecommunication system (UMTS) terrestrial radio access network (UTRAN). The
RNC controls the communication between the base station and the mobile station
30   based on predefined protocols, such as Radio Resource Control (RRC) or Medium
Access Control (MAC) or Radio Link Control (RLC) protocols. An example of a

2

controller node implemented in the core network (CN) side of the cellular network is a mobile switching center (MSC).

For example, in the 3rd generation UMTS a RNC can be connected further to a
5   serving GPRS support node (SGSN) which in turn is connected to a gateway or linking node, for example a gateway GPRS support node (GGSN) or gateway mobile switching center (GMSC), linking the cell to the other parts of the communication system and/or other communication networks, such as to a PSTN (Public Switched Telecommunications Network) or to a data network, such as to a
10   X.25 based network or to an IP (Internet Protocol) based network.

The wireless interface between the mobile station MS and the base station is typically controlled by only one access network controller at time. However, the MS may also be simultaneously controlled by several controller nodes. This may
15   occur e.g. when the cells overlap or in so called soft handoff mode, where the MS may be in communication with two base stations which may be connected to different controllers, or when one controller is controlling another controller controlling the MS. One controller of the plurality of controllers in the system can be defined as a serving (main) controller whereas the others may act as drift i.e.
20   secondary controllers.

The responsibility of controlling a connection between the mobile station and the network may change during an ongoing connection. It is therefore necessary to relocate at least part of the control functions associated with the connection from
25   one controller to another such that the connection will not become disconnected an/or that the quality of the connection remains in an acceptable level. When relocation is decided to be performed, the serving controller or another node of the communication system may initiate the necessary proceeding for the relocation. The relocation of the control function can be refereed to as handover.
30
For example, in the current third generation partnership project (3GPP) Specifications it is defined that the core network (CN) can request the UTRAN to

change the used ciphering and/or integrity protection keys for the air interface. This security procedure is initialised when the core network sends a radio access network application part (RANAP) message 'SECURITY MODE COMMAND' to the UTRAN. Based on this message the UTRAN, and more particularly, the

5   access network controller thereof shall initialise the corresponding security procedure for the air interface. From the CN point of view this security procedure has been completed when the CN receives the RANAP message 'SECURITY MODE COMPLETE' from the UTRAN. Based on this information the CN can be sure that either the new ciphering key has been taken into use for the air interface

10   or the mobile station has rejected the request for ciphering key change. The core network controller will also conclude from the acknowledgement message that the procedure has been terminated at the UTRAN side.

In the presently proposed arrangements the current i.e. ongoing security

15   procedure assumes that the earlier initialised security procedure has already been terminated when the serving RNC requests the core network controller to perform a serving radio network subsystem (SRNS) relocation, i.e. handover between two access network controllers. However, the inventors have found that this may not always be the case. For example, it is possible that the security procedure is not

20   completed if the defined activation time for the key change was originally defined to be a far a way from the current radio link controller sequence number (RLC SN) position. That is, the UTRAN keeps on operating with the "old" key until the timer functions indicates that it is time to change the key. In addition, since the reset procedures in the radio link controller (RLC) will start the transmission of frames

25   from the beginning (from frame No. 0), sequentially occurring RLC reset procedures may have continuously postponed the elapsing of the new ciphering key activation time. The reset procedures is initiated e.g. when the connection quality is found to become poor. Thus it is possible that the mobile station has already acknowledged the ciphering key exchange by sending the RRC

30   acknowledgement message 'SECURITY MODE COMPLETE' to the UTRAN (and which message the UTRAN has subsequently received) and that the new key activation time has not yet elapsed at the mobile station at the time when the

4

serving radio network subsystem relocation procedure is initialised. This is a problem since it may lead into situation where the mobile station and the new or target radio access network controller have different ciphering keys. It is then possible that the relocation procedure fails as the mobile station and the new radio

5   access network are not able to understand each other.

For example, the current RANAP message 'RELOCATION REQUIRED' contains the currently used ciphering key on the air interface inside a "IE: ciphering" key field. This field does not enable the serving RNC to indicate to the target RNC that

10   the earlier generated security procedure was not terminated before the SRNS relocation procedure was started. The inventors have realised that the serving RNC should be able to transmit to the target RNC also that ciphering key which was already agreed with the mobile station in addition to the currently used (i.e. the "old") ciphering key. This feature is, however, not supported in e.g. the current

15   third generation specifications. The current security modes may not be able to handle properly a situation where the new ciphering key has not yet been taken into a use due to "late" activation time and the serving controller is forced to initialise a relocation procedure. This may happen e.g. if the RRC message 'SECURITY MODE COMPLETE' has been received by the SRNC before the

20   initialisation of the SRNS relocation and before the activation timer at the mobile station has elapsed, i.e. while the mobile station and the currently serving RNC are still using the "old" key. The

Summary of the Invention

25

Embodiments of the present invention aim to address one or several of the above problems.

According to one aspect of the present invention, there is provided a method for

30   relocation from a first communication system controller to a second communication system controller of the control of communication between a first station and a second station, the communication being ciphered by means of a

5

first ciphering key, the method comprising: initiating relocation of control of the communication from the first controller to the second controller; and transmitting a request for relocation to the second controller, the request containing the first ciphering key and at least one other ciphering key.

5

According to another aspect of the present invention there is provided an arrangement in a communication system, comprising: a first entity for adapted control of communication between a first station and a second station, the communication being ciphered by means of a first ciphering key; a second entity

10 adapted for continuing the control of the communication after said communication has been changed to occur between a third station and the second station; an entity for initiating relocation of the control of the communication from the first entity to the second entity; and an entity for generating and transmitting a request for relocation to the second entity, the request containing the first ciphering key

15 and at least one other ciphering key.

According to a more specific embodiment the location request contains information regarding the timing when a ciphering key should be replaced by another key.

20 The embodiments of the invention may decrease the risk for disconnection of a ciphered connection during handover thereof from one access network controller to another. The transmission of data and/or signalling messages after the relocation may continue normally since in accordance with some embodiments the new controller may be made aware of ciphering key activation times for the radio

25 bearers and the new controller may therefore be made aware of the time when it should change the ciphering key for the radio interface. Some of the embodiments may avoid unnecessary initialisation of security procedures. The embodiments may prevent any additional delays to the start of the data transmission from the new controller to the mobile station. The embodiments may also be used to ensure

30 that the old and the new ciphering keys do not contradict when data transmission is initialised after the completion of the relocation procedure. The relocation may be made faster. This in turn may save radio resources since it the faster relocation

enables use of smaller power levels at the new base station. This in turn may decrease the interference caused for the other users in the new cell.

Brief Description of Drawings

5

For better understanding of the present invention, reference will now be made by way of example to the accompanying drawings in which:

Figure 1 shows three cells of a cellular system;

Figure 2 shows a part of a communication system where the preferred

10   embodiment of the present invention may be employed;

Figures 3 and 4 are flowcharts illustrating operation of two embodiments of the present invention.

Description of Preferred Embodiments of the Invention

15

Reference will be first made to Figure 1 in which three cells 1,2,3 of a cellular telecommunications network are shown. Each cell 1,2,3 is served by a respective base transceiver station (BTS) 4',4,5. Each base transceiver station (BTS) is arranged to transmit signals to and receive signals from the mobile stations (MS) 6

20   located in the cell associated with the given base transceiver station. Likewise, each mobile station 6 is able to transmit signals to and receive signals from the respective base transceiver station 4',4,5, and also able to move from the coverage area of one cell to the coverage area of another cell, e.g. from cell 2 to cell 3. When a mobile station moves such that the control of the wireless

25   communication between the mobile station and the network apparatus (i.e. the base stations) needs to be relocated from one access network controller to another, this is handled by handover proceedings.

- Reference is now made to Figure 2 which shows in more detail a part of a cellular

30   communication system. As can be seen, the mobile station 6 is in wireless communication with one of the base stations. Typically a number of mobile stations will be in communication with each base station although only one mobile

station is shown in Figure 2 for clarity. A first base station 4 is connected to a first network controller, which in Figure 2 is a serving radio network controller SRNC 10. More than one base station is usually connected to each access network controller although only one is shown for clarity. More than one controller may also

5   be provided in a UTRAN network subsystem. The SRNC 10 is connected to elements of the core network CN over an Iu interface 19. A RANAP (Radio Access Network Application Part; in the control plane) protocol can used for L3 (Layer 3) signalling over the Iu interface 19 between the RNCs 10, 11 and an appropriate controller element 14 of the core network CN. The core network element 14 can

10   be e.g. a mobile switching center MSC or a serving GPRS (General Packet radio Service)support node.

The RNC 10 is arranged to control the base station 4, either directly or through an intermediate node (not shown). The controller 10 passes on data to be transmitted

15   to the mobile station 6 by the base station. The controller 10 will also receive from the base station data which the base station has received from the mobile station. The implementation of the communication between the base station, the mobile station and the controller is known, and will thus not be discussed in detail herein. It is sufficient to note that the interface may comprise channels in both uplink and

20   downlink directions. The data may be sent between the mobile station and the controller in any suitable format. The messages sent from the mobile stations may include information identifying the mobile station (for instance, MS ID and/or IMSI (Mobile Station Identity and/or International Mobile Subscriber Identity, respectively)).

25
In addition to the serving controller (RNC 10), the cellular telecommunications system of Figure 2 includes another access network controller RNC 11 controlling the base station 5 of cell 3 of Figure 1. It is, again, noted that the second controller may also control more than one base station. The second controller may also

30   sometimes be referred to as a drift or target controller (DRNC or TRNC). The serving RNC may be referred to as source controller. The source RNC 10 and

target RNC 11 may have an open Iur interface 18 for communication between them.

Figure 2 illustrates one possible relocation situation wherein the mobile station MS
5   6 or similar user equipment communicates firstly via the BTS 4 over a radio interface designated by a solid line and then switches to communicate via a new BTS 5, as designated by the dashed radio interface. According to one possibility the change from one base station to another may occur after the mobile station 6 has moved into the service or illumination area of the second base station 5.
10   However, it is to be appreciated that in addition to the movement of the mobile station, there are also other possible reasons for triggering the relocation of the connection to another base station or to another network element, such as network optimization, load balancing, hardware congestion, connection quality improvement, fault in the system or base station and so on.
15
In order to ensure a proper operation of the system and to avoid disconnecting a possibly ongoing call, at least some of the functions of the network elements have to be relocated for the connection. For example, when a SRNC functionality is to be located from the first RNC 10 to the second RNC 11 at least some protocol
20   termination points of an ongoing connection (such as RRC, RCL and/or MAC protocols) may need to be changed from the first RNC to the second RNC.

The wireless communication, and more particularly, radio bearers (BR) between the base stations and the mobile station is ciphered by means of a ciphering key.
25   The use of different kinds of ciphering keys and techniques for ciphering data is known by the skilled person and will thus not be explained in more detail herein. The ciphering functions may be controlled by a control unit 20 at the serving controller 10 and by a control unit 21 at the target controller 11. The same controllers may be used for performing e.g. the RRC, RLC and MAC functions.
30   The new RNC needs also information regarding the used ciphering key The following describes in more detail an embodiment in which the serving RNC 10 is enabled to send the new and the currently used ciphering keys to the target RNC

11. In addition, it is also described how it is possible to transmit activation times that are defined for each radio bearer (RB) to the target RNC 11.

5   The relocation request, such as the RANAP 'RELOCATION REQUIRED' message, is typically transmitted from the UTRAN to the core network CN over the Iu interface when the serving RNS relocation procedure is to be initialised by the UTRAN. As explained above, the conventional relocation requests contain only the currently used ciphering key inside a predefined field, such as in the "IE: ciphering" key field. Therefore the serving RNC 10 is not capable to indicate to the target

10   RNC 11 that the mobile station will change the key after a certain period, for example since the earlier generated security procedure was not terminated before the serving RNS relocation procedure was started. Therefore the target RNC 11 may receive the "old" key which will not be used by the mobile station 6 after the timer function 7 thereof has triggered a change from the "old" key to a "new" key.

15

The handover procedure may be initiated by a 'HO_REQUIRED' message, which the RNC 10 sends to the MSC/SGSN 14. The message may comprise information necessary for setting up the handover, namely identification of the target RNC 11, possible identifiers for the Iur interface connections between RNC 10 and RNC 11,

20   and any necessary protocol control block information specifying the protocols and the current state of the protocols in use. Upon reception of the 'HO_REQUIRED' message the controller 14 starts to create new Iu connections to the target RNC 11. The core network controller 14 also sends a 'HO_REQUEST' message to RNC 11 over the Iu interface 19, which message includes the same information

25   necessary for setting up the handover at the target controller 11.

As shown by the flowchart of Figure 3, information of another ciphering key is added into the relocation request message. For example, a new "IE: new ciphering key" field may be added in the RANAP relocation request message. This new field

30   is used to indicate to the target RNC 11 that it should start using, instead of the current key, a new ciphering key for the air interface. The use of the new key may start immediately or after a predefined time. According to a preferred embodiment

10

shown in the Figure 4 flowchart the relocation request message includes also information regarding the timing of the change of keys. Possibilities for defining and transmission of the appropriate timing for the change will be explained later in this specification.

5

The new ciphering key field may also be used to indicate for the core network CN side that the timer setup for the security procedure shall be stopped for the duration of the serving RNS relocation procedure and that no new request for key changes, such as RANAP 'SECURITY MODE COMMAND' should be sent to the
10   serving RNC 10 during that time.

The new key field may be required only in instances where the termination of the security procedure has been interrupted by the serving RNS relocation procedure. Therefore it may be preferred to implement this field as an optional field in the
15   RANAP 'RELOCATION REQUIRED' message.

If the mobile station 6 has accepted the new ciphering key and the activation timing for the radio bearer (RB) upon the RRC security mode procedure, the mobile station expects the ciphering key to be changed when the activation time
20   expires. This may cause problems on the network side, because the current source RNC 10 should inform the target RNC 11 about the new ciphering key and the agreed activation time for it. Therefore it may be required that the serving RNC and the target RNC also exchange information regarding the agreed activation times for each radio bearer (RB) in addition to the information associated with the
25   different keys. Thus in the preferred embodiment mechanism the information between the source RNC 10 and the target RNC 11 comprises information of the new and the old ciphering keys and the agreed activation times of each radio bearers for the new ciphering key.

30   The activation time information was already sent to the mobile station 6 inside the RRC 'SECURITY MODE REQUEST' message, and therefore the mobile station assumes that the ciphering key is going to be changed based on the agreed

11

activation times. Upon the serving RNS relocation procedure this information may
be sent to the target RNC 11 inside the RRC initialisation information (for more
information about this feature, see e.g. 3GTS 25.331, chapter 14.10). The RRC
initialisation information contains a set of parameters on which the target RNC 11

5   may base the configuration of e.g. the radio resource control protocol (RRC),
medium access control protocol (MAC), radio link control protocol (RLC), and/or
packet data convergence protocol (PDCP) entities.

According to a possibility the timing is indicated by a data frame sequence

10   number. That is, the information includes the number of the frame from which on
(either including the indicated data frame or from the next one) the ciphering key
should be changed. A possibility is to add a separate RLC sequence number field
into the relocation request information. One field is preferably added for each radio
bearer from the corresponding CN domain. This field may then be used to indicate

15   to the target RNC 11 the RLC sequence number from which on the new ciphering
key shall be taken into a use. In other words, to indicate the time when the given
activation times for the RB(s) elapse at the mobile station.

It should be appreciated that it is possible to transmit information about more than

20   two keys between the controllers. This may be required e.g. if several keys are
used simultaneously for communication between the mobile station and the base
station (e.g. for simultaneous voice and data calls) or when several subsequent
relocations and/or security mode request have lead to a situation where it is
possible that several different possible keys exist at the same time.

25

In an embodiment initialisation of the SRNS relocation procedure is forbidden until
a RANAP message 'SECURITY MODE COMPLETE' has been sent to the core
network. It is also possible that before the initialisation of the SRNS relocation
procedure the serving RNC repeats the security procedure for the air interface and

30   advances the activation time for the new ciphering key by sending the new
activation time to the mobile station. After this the RNC waits until the new
ciphering has been taken into a use in order to send the RANAP message

12

'SECURITY MODE COMPLETE' to the core network. According to a still further possibility a new RRC message is created for calling the previously generated security procedure off. The SRNS relocation procedure can be initialised after the mobile station has acknowledged this message.

5

It should be appreciated that whilst embodiments of the present invention have been described in relation to mobile stations, embodiments of the present invention are applicable to any other suitable type of user equipment.

10 The exemplifying cellular telecommunications network has been described by using the terminology of a proposed Universal Mobile Telecommunications System (UMTS) standard. However, it is to be appreciated that the invention is not restricted to UMTS but can be implemented in any standard. Examples of these include, without any intention to restrict the possible communication systems to

15 these, any of the code division multiple access (CDMA) based systems or any of the time division multiple access (TDMA) based systems or any of the frequency division multiple access (FDMA) based systems or any hybrids thereof.

It should also be appreciated that base stations can sometimes be referred to as

20 node B. In addition, the term cell is intended to cover also a group of cells in instances where more than one cell is controlled by a controller entity (for instance a URA update).

The above discusses the transfer of information between two radio network

25 controllers and the between the radio network controller and the core network controller. Embodiments of the present invention can be applicable to other network elements where applicable.

It is also noted herein that while the above describes exemplifying embodiments of

30 the invention, there are several variations and modifications which may be made to the disclosed solution without departing from the scope of the present invention as defined in the appended claims.

Claims

1.   A method for relocation from a first communication system controller to a second communication system controller of the control of communication between a first station and a second station, the communication being ciphered by means of a first ciphering key, the method comprising:

initiating relocation of control of the communication from the first controller to the second controller; and

transmitting a request for relocation to the second controller, the request containing the first ciphering key and at least one other ciphering key.

2.   A method as claimed in claim 1, comprising a step subsequent to the said transmitting step of the second controller to cipher communication with the second station by means of the said other ciphering key.

3.   A method as claimed in claim 1 or 2, comprising the step of the second station ciphering communication by means of the said other ciphering key without intervention from the second controller.

4.   A method as claimed in claim 3, comprising the step prior to the said transmitting step of the first controller transmitting to the second station a cipher request requesting the second station to cipher communication with the first station by means of the said other key.

5.   A method as claimed in claim 4, wherein the second station is arranged to, in response to the said cipher request, begin to cipher communication with the first station by means of the said other key after a delay.

6.   A method as claimed in claim 5, wherein the request for relocation includes data indicative of at least one point after which the communication with the first station is to be ciphered by means of the said other key.

14

7.   A method as claimed in claim 6 as dependant on claim 2, wherein the second controller controls a third station to begin ciphering communication with the second station by means of the said other ciphering key at the point indicated in the request for relocation.

5

8.   A method as claimed in any preceding claim, wherein the location request contains an additional field for transferring information of the said other key.

9.   A method as claimed in claim 8, wherein the additional field is optional.

10

10.   A method as claimed in any preceding claim, wherein the request for relocation comprises a relocation request message based on a radio access network application part protocol.

15   11.   A method as claimed in any preceding claim, wherein the request for relocation contains information regarding activation times of the said at least one other key for each radio bearer to be relocated under control of the second controller.

20   12.   A method as claimed in claim 11, wherein the information of the activation times is included in radio resource control initialisation information.

13.   A method as claimed in any of claims 6 to 12, wherein the request for relocation contains the sequence number of a data frame from which on the said

25   other key is to be used for the ciphering of the communication.

14.   A method as claimed in claim 13, wherein the request for relocation contains a sequence number field for each radio bearer to be relocated from the first controller.

30

15.   A method as claimed in claim 13 or 14, wherein the sequence number comprises a radio link control protocol sequence number.

15

16.   A method as claimed in any preceding claim, wherein the request for
relocation is transmitted from the first controller to a core network controller, the
core network controller transmits a relocation request to the second controller, and
5   the core network controller will disable any security procedures requiring a change
of the ciphering keys for the duration of the relocation procedures in response to
the request from the first controller.

17.   A method as claimed in any preceding claim, wherein the first station is a
10   base station of a cellular communication system, the second station is a mobile
station, and the first and second controllers are radio access network controllers of
the cellular communication system.

18.   An arrangement in a communication system, comprising:
15   a first entity for adapted control of communication between a first station
and a second station, the communication being ciphered by means of a first
ciphering key;
          a second entity adapted for continuing the control of the communication
after said communication has been changed to occur between a third station and
20   the second station;
          an entity for initiating relocation of the control of the communication from the
first entity to the second entity; and
          an entity for generating and transmitting a request for relocation to the
second entity, the request containing the first ciphering key and at least one other
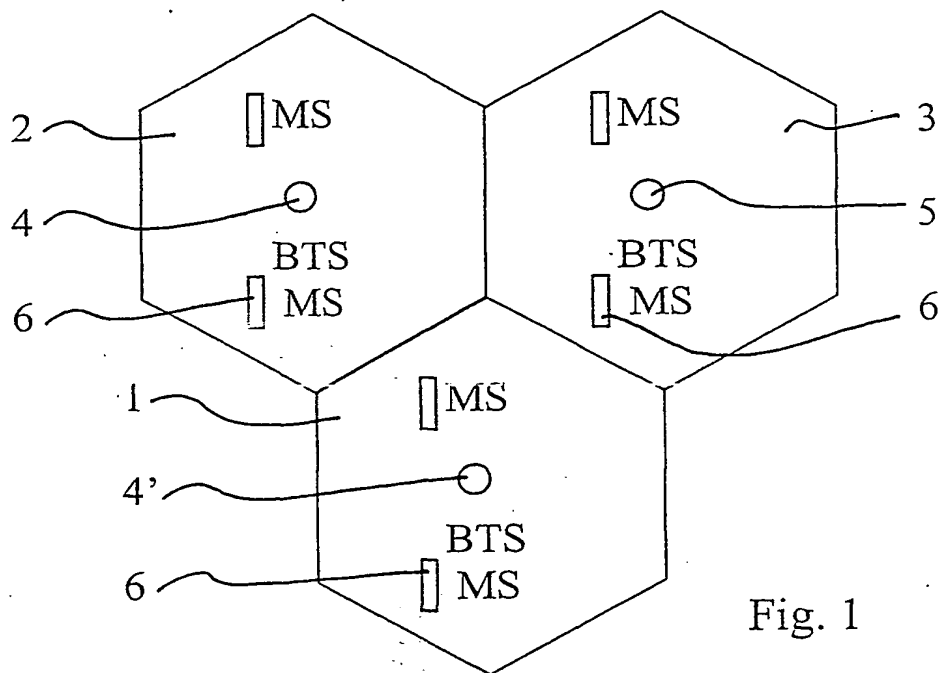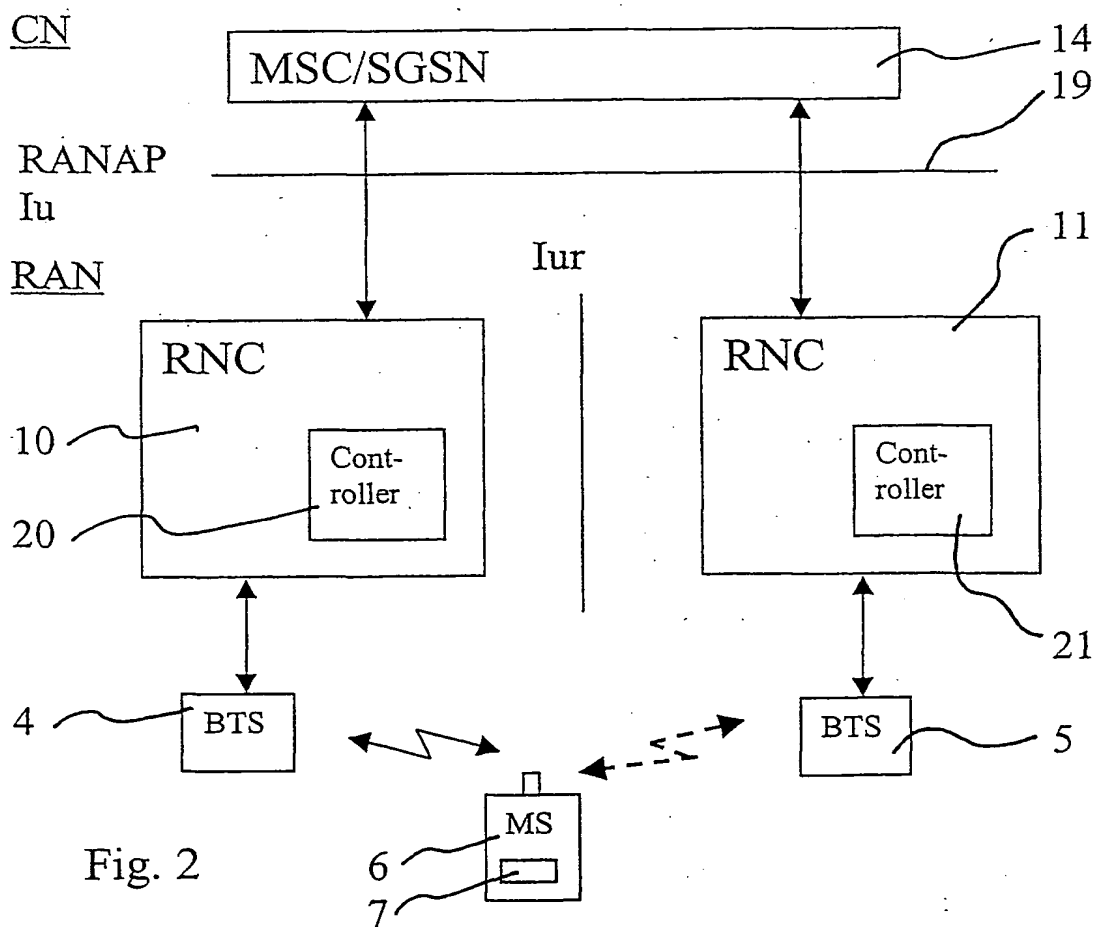25 .   ciphering key.

Fig. 1

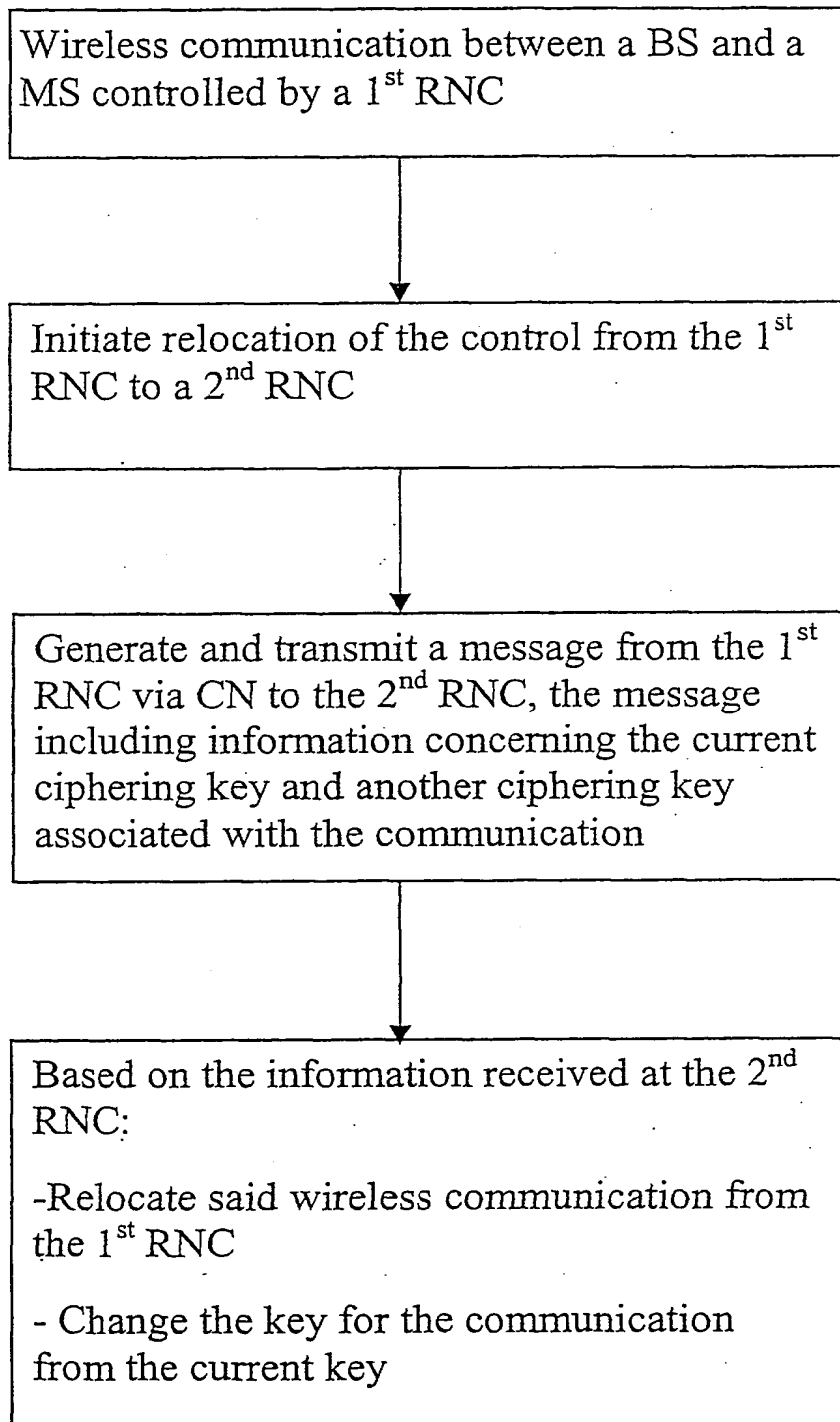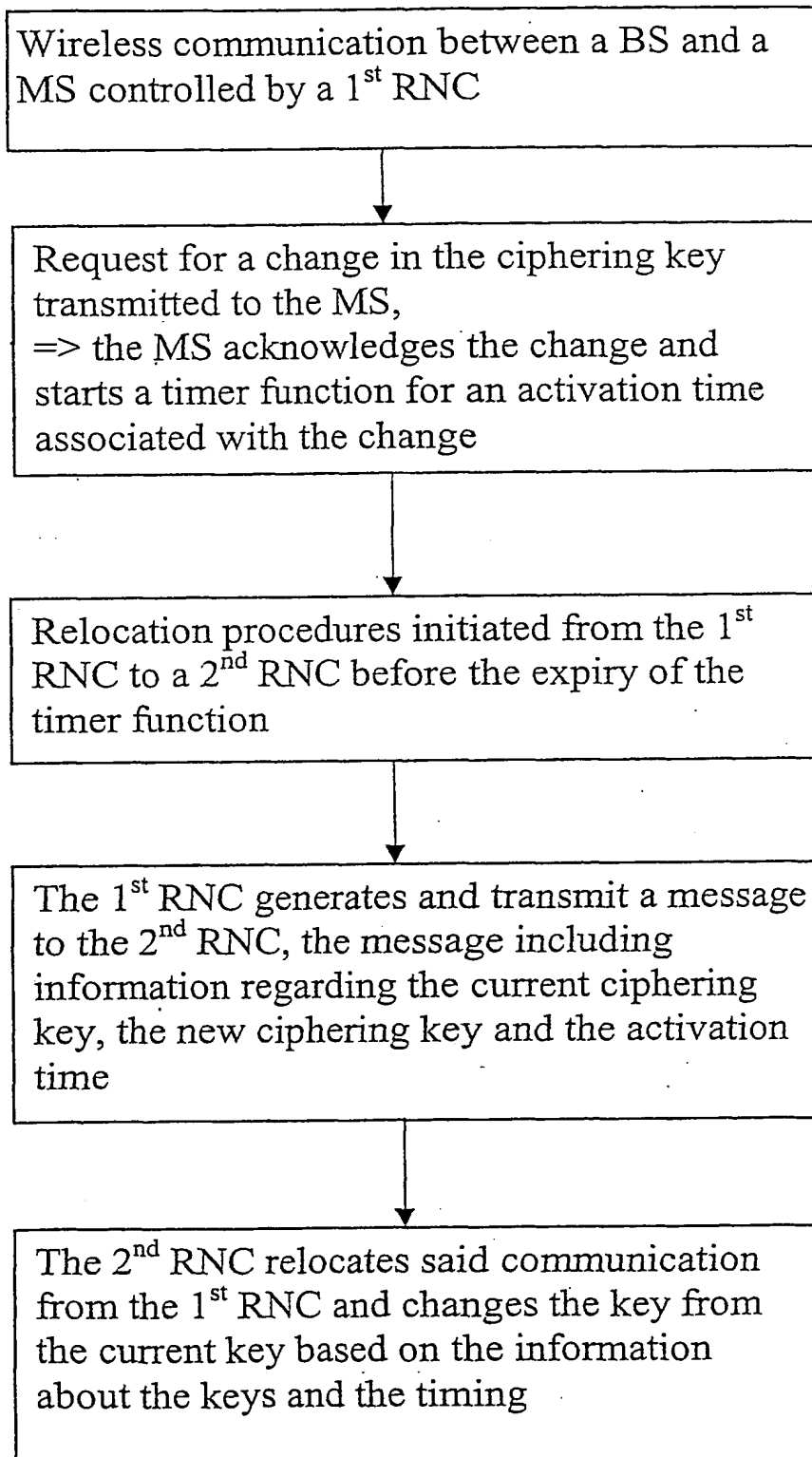Fig. 2

Wireless communication between a BS and a
MS controlled by a 1st RNC

Initiate relocation of the control from the 1st
RNC to a 2nd RNC

Generate and transmit a message from the 1st
RNC via CN to the 2nd RNC, the message
including information concerning the current
ciphering key and another ciphering key
associated with the communication

Based on the information received at the 2nd
RNC:

-Relocate said wireless communication from
the 1st RNC

- Change the key for the communication
from the current key

Fig. 3

Fig. 4

(51) International Patent Classification⁷: H04Q 7/38

(21) International Application Number: PCT/EP01/08856

(22) International Filing Date: 31 July 2001 (31.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0020443.8   18 August 2000 (18.08.2000)   GB

(71) Applicant (for all designated States except US): NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and
(75) Inventors/Applicants (for US only): ISOKANGAS, Jari [FI/FI]; Itsenäisyydenkatu 8 C 43, FIN-33500 Tampere (FI). SARKKINEN, Sinikka [FI/FI]; Kisällinkuja 5, FIN-36200 Kangasala (FI).

(74) Agents: RUUSKANEN, Juha-Pekka et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

[Continued on next page]
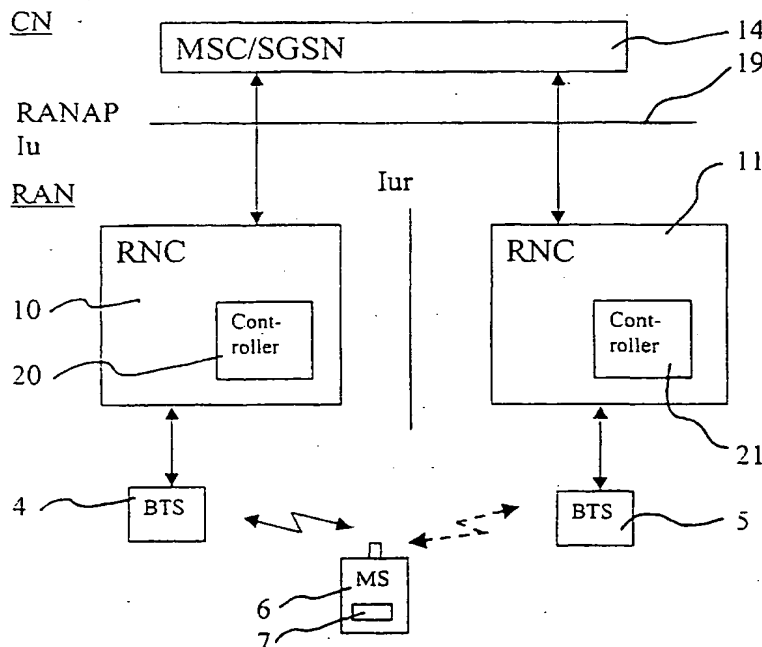
(54) Title: CONTROLLING COMMUNICATIONS BETWEEN STATIONS

(57) Abstract: The present invention relates to relocation of the control of communication between a first station and a second station from a first communication system controller to a second communication system controller. The communication is ciphered by means of a first ciphering key. In the method, after the initiation of the relocation of control of the communication from the first controller to the second controller a request for relocation is transmitted to the second controller. The request contains the first ciphering key and at least one other ciphering key.

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(88) Date of publication of the international search report:
6 June 2002

IN RNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7   H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 00 36860 A (NOKIA NETWORKS OY.) 22 June 2000 (2000-06-22) abstract; figures 4,5,8 page 10, line 5 -page 11, line 25	1,18
A	*IDEM*	2-17
Y	ETSI: "TS 125 413 Universal Mobile Telecommunications System (UMTS);UTRAN Iu Interface RANAP Signalling (3G TS 25.413 Version 3.0.0 Release 1999)" ETSI TS 125 413 V3.0.0, XX, XX, January 2000 (2000-01), pages 1-147, XP002165163 paragraph '9.2.1.28!	1,18
A	*IDEM*	2-17

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 March 2002	04/04/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Danielidis, S

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document. with indication.where appropriate. of the relevant passages	Relevant to claim No.
A	WO 99 51051 A (NOKIA TELECOMMUNICATIONS OY.) 7 October 1999 (1999-10-07) abstract; claim 1; figures 2-5 -----	1

1

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0036860	A	22-06-2000	FI	990757 A	17-06-2000
			AU	1661900 A	03-07-2000
			CN	1330841 T	09-01-2002
			EP	1142391 A1	10-10-2001
			WO	0036860 A1	22-06-2000
WO 9951051	A	07-10-1999	FI	980736 A	01-10-1999
			AU	3149699 A	18-10-1999
			BR	9909307 A	21-11-2000
			CN	1297664 T	30-05-2001
			EP	1068757 A2	17-01-2001
			WÜ	9951051 A2	07-10-1999

THIS PAGE BLANK (USPTO)